Boletín de julio de 2019

Avisos Técnicos

Múltiples vulnerabilidades en productos de IBM

Fecha de publicación: 01/07/2019

Importancia: Crítica

Recursos afectados:

- IBM Spectrum Protect Plus, versión 10.1.3 y anteriores;
- IBM Spectrum Protect y Storage Agents:
  - Versiones desde la 8.1.0.0 hasta la 8.1.7.xxx;
  - Versiones desde la 7.1.0.0 hasta la 7.1.9.200;
- IBM Cognos TM1, versión 10.2.2.

Descripción:

IBM ha detectado múltiples vulnerabilidades, de las cuales, una es de severidad crítica, cuatro son altas y una de severidad media.

Solución:

- IBM Spectrum Protect Plus, actualizar a la versión 10.1.4;
- IBM Spectrum Protect y Storage Agents:
  - Rama 8.1, actualizar a la versión 8.1.8;
  - Rama 7.1, actualizar a la versión 7.1.9.300;
- IBM Cognos TM1 10.2.2, aplicar el parche de seguridad Cognos TM1 10.2.2.7 Interim Fix 22.

Detalle:

- La vulnerabilidad de severidad crítica en IBM Spectrum Protect y Storage Agents se debe a un desbordamiento de búfer basado en pila. Un atacante remoto podría ejecutar código arbitrario con los privilegios de identidad de la instancia o bloquear el sistema. Se ha reservado el identificador CVE-2019-4087 para esta vulnerabilidad.
- Una vulnerabilidad de criticidad alta en IBM Spectrum Protect y Storage Agents se debe a la carga en el módulo *dsmqsan* de una librería especialmente creada. Un atacante local podría obtener privilegios de *root* en el sistema. Se ha reservado el identificador CVE-2019-4088 para esta vulnerabilidad.
- Una vulnerabilidad de criticidad alta en IBM Cognos TM1 se debe a llamadas inseguras de las funciones *CreateProcess()* y *CreateProcessAsUser()* al usar rutas de búsquedas sin entrecomillar en Windows. Un atacante local podría ejecutar código arbitrario con escalada de privilegios. Se ha reservado el identificador CVE-2019-4245 para esta vulnerabilidad.
- Una vulnerabilidad de criticidad alta en IBM Spectrum Protect Plus se debe, cuando este es empleado, para proteger bases de datos Oracle o MongoDB. Un atacante podría realizar una escalada de privilegios. Se ha reservado el identificador CVE-2019-4383 para esta vulnerabilidad.
- Una vulnerabilidad de criticidad alta en IBM Spectrum Protect Plus se debe, cuando este es empleado, para proteger bases de datos Oracle, DB2 o MongoDB. Un atacante podría ejecutar código arbitrario en el sistema. Se ha reservado el identificador CVE-2019-4357 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad

Inundación de certificados en OpenPGP

Fecha de publicación: 01/07/2019

Importancia: Crítica

Recursos afectados:

- Certificados OpenPGP alojados en la red de servidores de claves SKS.

Descripción:

Robert J. Hansen y Daniel Kahn Gillmor, han comunicado múltiples vulnerabilidades en OpenPGP debido a un fallo en el diseño de "solo escritura" de los servidores de claves SKS que podrían provocar la denegación del servicio.

Solución:

- No utilizar la red de servidores de claves SKS para actualizar certificados OpenPGP. En su lugar, usar un servidor alternativo como, por ejemplo, keys.openpgp.org.
- Eliminar del llavero los certificados públicos envenenados y adquirirlos, nuevamente, desde un canal confiable.

Detalle:

SKS es vulnerable a ataques de inundación de certificados como consecuencia de su diseño de solo escritura. Esto podría permitir a un atacante envenenar certificados OpenPGP, añadiendo una gran cantidad de firmas "spam" que no pueden ser eliminadas. El envenenamiento hace que GnuPG no pueda importar certificados desde los servidores de claves SKS, provocando la denegación del servicio.

Etiquetas: Vulnerabilidad

Múltiples vulnerabilidades en iDRAC de Dell EMC

Fecha de publicación: 02/07/2019

Importancia: Alta

Recursos afectados:

- Dell EMC iDRAC6, versiones anteriores a 2.92;
- Dell EMC iDRAC7/iDRAC8, versiones anteriores a 2.61.60.60;
- Dell EMC iDRAC9, versiones anteriores a:
  - 3.20.21.20;
  - 3.21.24.22;
  - 3.21.25.22;
  - 3.21.26.22;
  - 3.22.22.22;
  - 3.23.23.23;
  - 3.24.24.24;
  - 3.30.30.30.

Descripción:

Dell EMC ha detectado tres vulnerabilidades de criticidad alta en múltiples productos de la familia iDRAC. Un atacante remoto podría, ejecutar código arbitrario, saltarse la autenticación o bloquear el sistema.

Solución:

- Actualizar el firmware de iDRAC9 a la versión:
  - 3.20.21.20;
  - 3.21.24.22;
  - 3.21.25.22;
  - 3.21.26.22;
  - 3.22.22.22;
  - 3.23.23.23;
  - 3.24.24.24;
  - 3.30.30.30.
- Actualizar el firmware de iDRAC8 e iDRAC7 a la versión 2.61.60.60.
- Actualizar el firmware de iDRAC6 a la versión 2.92.

Detalle:

- Una vulnerabilidad se debe a un desbordamiento de búfer basado en pila. Un atacante remoto podría ejecutar código arbitrario, con privilegios de *webserver*, o detener el sistema. Se ha asignado el identificador CVE-2019-3705 para esta vulnerabilidad.
- Una vulnerabilidad se debe al envío de datos, especialmente creados, a la interfaz web de iDRAC. Un atacante remoto podría realizar un salto de autenticación en el sistema. Se ha asignado el identificador CVE-2019-3706 para esta vulnerabilidad.
- Una vulnerabilidad se debe al envío de datos de entrada, especialmente creados, a la interfaz WS-MAN. Un atacante remoto podría realizar un salto de autenticación en el sistema. Se ha asignado el identificador CVE-2019-3707 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos de F5

Fecha de publicación: 02/07/2019

Importancia: Alta

Recursos afectados:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), versiones:
  - 14.0.0 - 14.1.0.5;
  - 13.0.0 - 13.1.1.4;
  - 12.1.0 - 12.1.4;
  - 11.5.1 - 11.6.4.
- F5 SSL Orchestrator, versiones:
  - 14.0.0;
  - 14.1.0.

Descripción:

F5 ha publicado múltiples vulnerabilidades del tipo XSS, DoS, inyección de comandos y flujo de tráfico no revelado.

Solución:

Actualizar a las siguientes versiones:

- BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator):
  - 15.0.0;
  - 14.1.0.6;
  - 13.1.1.5;
  - 12.1.4.1;
  - 11.6.4;
  - 11.5.9.
- F5 SSL Orchestrator:
  - 15.0.0;
  - 14.1.0.6.

Detalle:

- Existen vulnerabilidades de tipo *cross-site scripting* (XSS) reflejado en una página no revelada de *Traffic Management User Interface* (TMUI), también conocida como la utilidad de configuración, que permitiría a un atacante ejecutar comandos con privilegios de administrador. Se han reservado los identificadores CVE-2019-6625 y CVE-2019-6626 para estas vulnerabilidades.
- Un atacante remoto puede ser capaz de interrumpir el servicio, causando un reinicio de *Traffic Management Microkernel* (TMM). Este problema solo afecta a los sistemas F5 SSL Orchestrator que realizan encadenamiento transparente de *proxy* con SNAT habilitado. Se han reservado los identificadores CVE-2019-6627 y CVE-2019-6630 para esta vulnerabilidad.
- iControl REST *worker* no revelado es vulnerable a la inyección de comandos por parte de un usuario con privilegios de administrador. Este problema afecta tanto a las implementaciones de iControl REST, como a las de tmsh. Se han reservado los identificadores CVE-2019-6620, CVE-2019-6621 y CVE-2019-6622 para esta vulnerabilidad.
- El tráfico no revelado, enviado al servidor virtual BIG-IP iSession, puede causar que *Traffic Management Microkernel* (TMM) se reinicie, causando una denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-6623 para esta vulnerabilidad.
- Un atacante remoto puede hacer que *Traffic Management Microkernel* (TMM) se reinicie, consiguiendo una denegación de servicio (DoS) en el sistema vulnerable. Se ha reservado el identificador CVE-2019-6624 para esta vulnerabilidad.
- En un sistema BIG-IP PEM configurado para alta disponibilidad (HA), y bajo ciertas condiciones, el proceso TMM puede finalizar y reiniciarse mientras se procesa el tráfico BIG-IP PEM con OpenVPN classifier. Se ha reservado el identificador CVE-2019-6628 para esta vulnerabilidad.
- El procesamiento del tráfico se interrumpe mientras se reinicia *Traffic Management Microkernel* (TMM). Si el dispositivo F5 afectado se configura como parte de un grupo de dispositivos, el sistema activará una conmutación por error en el dispositivo paritario. Se ha reservado el identificador CVE-2019-6629 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en productos Cisco

Fecha de publicación: 04/07/2019

Importancia: Alta

Recursos afectados:

- Cisco AsyncOS Software para Cisco Web Security Appliance (WSA), tanto para dispositivos virtuales, como para hardware, cuando los dispositivos tienen habilitada la función de proxy HTTPS y tienen configurada al menos una política de descifrado.
- Cisco Small Business 200, 300, y 500 Series Managed Switches, que ejecuten versiones de software anteriores a la 1.4.10.6 con la interfaz web de administración habilitada o configurada para permitir HTTPS.
- Cisco Enterprise NFV Infrastructure Software (NFVIS), versiones anteriores a 3.10.1.
- Cisco Nexus 9000 Series Fabric Switches en modo ACI, que ejecuten una versión de software anterior a 14.1(2g) y utilizando la configuración por defecto de fábrica del modo permisivo.
- Cisco Jabber para Windows, versiones anteriores a 12.6(0).
- Cisco Unified Communications Manager.
- Cisco APIC Software, versiones anteriores a 4.1(2g).

Descripción:

Cisco ha publicado diez vulnerabilidades de criticidad alta. Un atacante podría realizar ataques de denegación de servicio (DoS), corrupción de memoria, lectura o escritura de archivos arbitrarios, inyección de comandos, acceso no autorizado, precarga de DLL y escalada de privilegios.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde el panel de descarga de software de Cisco.

Detalle:

Las vulnerabilidades se deben a:

- Validación insuficiente de los certificados de servidor *Secure Sockets Layer* (SSL) en la función de descifrado HTTPS. Un atacante remoto, no autenticado, podría provocar una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-1886 para esta vulnerabilidad.
- Validación incorrecta en el procesador de entrada de paquetes HTTPS. Un atacante remoto, no autenticado, podría provocar una corrupción de memoria en un dispositivo afectado. Se ha reservado el identificador CVE-2019-1892 para esta vulnerabilidad.
- Validación incorrecta de las solicitudes enviadas a la interfaz web. Un atacante remoto, no autenticado, podría provocar una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-1891 para esta vulnerabilidad.
- Validación de entrada incorrecta en los comandos del sistema de archivos NFVIS. Un atacante remoto, autenticado, y con privilegios de administrador podría sobrescribir o leer archivos arbitrarios en el sistema operativo subyacente. Se ha reservado el identificador CVE-2019-1894 para esta vulnerabilidad.
- Validación insuficiente de entrada de un archivo de configuración que es accesible para un usuario local de la *shell*. Un atacante local, autenticado como *root*, podría ejecutar comandos arbitrarios en el sistema operativo. Se ha reservado el identificador CVE-2019-1893 para esta vulnerabilidad.
- Requisitos de seguridad insuficientes durante la fase de configuración del *Link Layer Discovery Protocol* (LLDP) de la infraestructura VLAN. Un atacante adyacente, no autenticado, podría eludir las validaciones de seguridad y conectar un servidor no autorizado a la VLAN de la infraestructura. Se ha reservado el identificador CVE-2019-1890 para esta vulnerabilidad.
- Validación insuficiente de los recursos cargados por la aplicación en tiempo de ejecución. Un atacante local, autenticado, podría

realizar un ataque de precarga de DLL. Se ha reservado el identificador CVE-2019-1855 para esta vulnerabilidad.
- Validación insuficiente del tráfico SIP de entrada. Un atacante remoto, no autenticado, podría causar una condición de denegación de servicio (DoS). Se ha reservado el identificador CVE-2019-1887 para esta vulnerabilidad.
- Validación y comprobación de errores incompletas de la ruta del archivo cuando se carga un software específico. Un atacante remoto, autenticado, podría escalar privilegios y obtener permisos de *root* en un dispositivo afectado. Se ha reservado el identificador CVE-2019-1889 para esta vulnerabilidad.
- Mecanismos de validación de entrada insuficientes para determinados campos de las peticiones HTTP/HTTPS enviadas a través de un dispositivo afectado. Un atacante remoto, autenticado, podría provocar una condición de denegación de servicio (DoS) en un dispositivo afectado. Se ha reservado el identificador CVE-2019-1884 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad en UIoT de HPE

Fecha de publicación: 08/07/2019

Importancia: Alta

Recursos afectados:

- HPE Universal Internet of Things (UIoT), versiones:
  - 1.6;
  - 1.5;
  - 1.4.2;
  - 1.4.1;
  - 1.4.0;
  - 1.2.4.2.

Descripción:

HPE ha detectado una vulnerabilidad de criticidad alta en múltiples versiones de UIoT.

Solución:

- Versiones de UIoT 1.6, actualizar a la versión 1.6 RP603.
- Versiones de UIoT 1.5, actualizar a la versión 1.5 RP503 HF3.
- Versiones anteriores a UIoT 1.5, como en los casos de UIoT 1.4.0, 1.4.1, 1.4.2 y 1.2.4.2, actualizar a las versiones 1.5 RP503 HF3 o 1.6 RP603.

Detalle:

La vulnerabilidad en UIoT podría permitir a un atacante remoto acceder sin autorización al dispositivo, o a información sensible. Se ha reservado el identificador CVE-2019-11990 para esta vulnerabilidad.

Etiquetas: Actualización, HP, IoT, Vulnerabilidad

Vulnerabilidad en 3PAR Service Processor de HPE

Fecha de publicación: 09/07/2019

Importancia: Crítica

Recursos afectados:

HPE 3PAR Service Processor (SP), versiones desde la 4.1 hasta la 4.4.

Descripción:

HPE ha detectado una vulnerabilidad de severidad crítica en múltiples versiones de 3PAR Service Processor que podría permitir la interrupción de la confidencialidad, integridad y disponibilidad.

Solución:

- Actualizar a la versión 4.4 MU9 (SP-4.4.0.GA-142) de HPE 3PAR Service Processor.
- Si la versión actual del sistema operativo 3PAR no es 3.2.2EMU4 o 3.2.2MU6, consultar la matriz de soporte de actualización de 3PAR para actualizar el Service Processor y el sistema operativo de HPE 3PAR.

Detalle:

HPE 3PAR Service Processor tiene una vulnerabilidad de divulgación remota de información, que podría permitir a un atacante la interrupción de la confidencialidad, integridad y disponibilidad del Service Processor y de cualquier *array* 3PAR administrado. Se ha reservado el identificador CVE-2019-11991 para esta vulnerabilidad.

Etiquetas: Actualización, HP, Vulnerabilidad

Boletín de seguridad de Microsoft de julio de 2019

Fecha de publicación: 10/07/2019

Importancia: Crítica

Recursos afectados:

- Microsoft Windows,
- Internet Explorer,
- Microsoft Edge,
- Microsoft Office and Microsoft Office Services and Web Apps,
- Azure DevOps,
- Open Source Software,
- .NET Framework,
- Azure,
- SQL Server,
- ASP.NET,
- Visual Studio,
- Microsoft Exchange Server.

Descripción:

La publicación de actualizaciones de seguridad de Microsoft correspondiente al mes de julio consta de 75 vulnerabilidades, 15 clasificadas como críticas y 60 como importantes.

Solución:

Instalar la actualización de seguridad correspondiente. En la página de información de la instalación de las mismas actualizaciones, se informa de los distintos métodos para llevarlas a cabo.

Detalle:

Las vulnerabilidades publicadas se corresponden con los siguientes tipos:

- Ejecución remota de código,
- Divulgación de información,
- Elevación de privilegios,
- Denegación de servicio,
- Evasión de seguridad,
- Suplantación.

Etiquetas: Actualización, Microsoft, Vulnerabilidad

Vulnerabilidad en Intel® Processor Diagnostic Tool

Fecha de publicación: 10/07/2019

Importancia: Alta

Recursos afectados:

- Intel® Processor Diagnostic Tool para 32-bit, versiones anteriores a la 4.1.2.24_32bit.
- Intel® Processor Diagnostic Tool para 64-bit, versiones anteriores a la 4.1.2.24_64bit.

Descripción:

Se ha publicado una vulnerabilidad en Intel® Processor Diagnostic Tool que podría permitir a un atacante la escalada de privilegios, la denegación de servicio o la divulgación de información.

Solución:

Actualizar a Intel® Processor Diagnostic Tool versión 4.1.2.24 o posterior.

Detalle:

Un control de acceso inadecuado en la herramienta de diagnóstico del procesador Intel(R) anterior a la versión 4.1.2.24 podría permitir a un usuario autenticado la escalada de privilegios, la divulgación de información o la denegación de servicio a través del acceso local. Se ha reservado el identificador CVE-2019-11133 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de SAP de julio de 2019

Fecha de publicación: 10/07/2019

Importancia: Crítica

Recursos afectados:

- SAP Diagnostic Agent (LM-Service), versión 7.20.
- Tests de SAP NetWeaver Process Integration ABAP (SAP Basis), versiones 7.0, 7.1, 7.3, 7.31, 7.4 y 7.5.
- SAP Commerce Cloud (ex SAP Hybris Commerce) (HY_COM), versiones 6.3, 6.4, 6.5, 6.6, 6.7, 1808 y 1811.
- OpenUI5, versiones anteriores e incluyendo 1.38.39, 1.44.39, 1.52.25, 1.60.6 y 1.63.0.
- SAP Information Steward, versión 4.2.
- ABAP Server y ABAP Platform (SAP Basis), versiones 7.31, 7.4 y 7.5.
- SAP BusinessObjects Business Intelligence Platform (BI Workspace) (Enterprise), versiones 4.1, 4.2 y 4.3.
- SAP NetWeaver para Java Application Server (Web Container), versiones de *engineapi* (7.1, 7.2, 7.3, 7.31, 7.4 y 7.5) y de *servercode* (7.2, 7.3, 7.31, 7.4 y 7.5).
- SAP ERP HCM (SAP_HRCES), versión 3.
- SAP NetWeaver Application Server para Java (Startup Framework), versiones 7.21, 7.22, 7.45, 7.49, y 7.53.
- SAP Gateway, versiones 7.5, 7.51, 7.52 y 7.53.

Descripción:

SAP ha publicado varias actualizaciones de seguridad de diferentes productos en su comunicado mensual.

Solución:

Visitar el portal de soporte de SAP e instalar las actualizaciones o los parches necesarios, según indique el fabricante.

Detalle:

SAP, en su comunicación mensual de parches de seguridad, ha emitido un total de 11 notas de seguridad, siendo 1 de ellas de severidad crítica, 1 alta y 9 medias.

El tipo de vulnerabilidades publicadas se corresponde a los siguientes:

- 4 vulnerabilidades de *Cross-Site Scripting* (XSS).
- 1 vulnerabilidad de inyección de código.
- 1 vulnerabilidad de inyección de comandos del sistema operativo.
- 1 vulnerabilidad de denegación de servicio.
- 1 vulnerabilidad de divulgación de información.
- 3 vulnerabilidades de otro tipo.

Las notas de seguridad calificadas como crítica y alta se refieren a:

- Se ha identificado una vulnerabilidad crítica en SolMan Diagnostic Agent (SMDAgent), perteneciente a Solution Manager (SolMan), encargado de gestionar las comunicaciones de eventos de monitorización y diagnóstico entre cada sistema SAP y el Solution Manager. Esta vulnerabilidad permitiría a un atacante comprometer el sistema SAP por completo. Se ha reservado el identificador CVE-2019-0330 para esta vulnerabilidad.
- En la herramienta Extended Computer Aided Test Tool (eCATT), utilizada para la realización de pruebas de *testing* automatizadas, se ha encontrado una vulnerabilidad de severidad alta que permitiría realizar una inyección de código, impactando en la integridad y disponibilidad del sistema. Se ha reservado el identificador CVE-2019-0328 para esta vulnerabilidad.

Etiquetas: Actualización, SAP, Vulnerabilidad

Denegación de servicio en controlador criptográfico TLS y SSL de Cisco ASA y FTD

Fecha de publicación: 11/07/2019

Importancia: Alta

Recursos afectados:

- ASA 5506-X,
- ASA 5506-X con FirePOWER Services,
- ASA 5506H-X,
- ASA 5506H-X con FirePOWER Services,
- ASA 5506W-X,
- ASA 5506W-X con FirePOWER Services,
- ASA 5508-X,
- ASA 5508-X con FirePOWER Services,
- ASA 5516-X,
- ASA 5516-X con FirePOWER Services.

La vulnerabilidad se aplica solo a las plataformas de hardware ASA que utilizan un controlador criptográfico específico para el cifrado y descifrado de paquetes SSL y TLS. Hay múltiples características que, cuando se habilitan, hacen que el software Cisco ASA o FTD procese paquetes SSL/TLS. Estas características incluyen, entre otras:

- AnyConnect y Clientless SSL VPN,
- HTTP server utilizado para la interfaz de gestión.

Descripción:

Una vulnerabilidad en el controlador criptográfico para el software Cisco Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD) podría permitir que un atacante remoto, no autenticado, reinicie el dispositivo de forma inesperada.

Solución:

Las actualizaciones que corrigen las vulnerabilidades indicadas pueden descargarse desde: Panel de descarga de Software Cisco.

Detalle:

- La validación de entrada insuficiente de un encabezado de paquete de entrada de Secure Sockets Layer (SSL) o Transport Layer Security (TLS) podría permitir a un atacante enviar un paquete TLS/SSL creado a una interfaz en el dispositivo de destino, recargando el dispositivo, lo que resultaría en una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2019-1873 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Múltiples vulnerabilidades en Citrix SD-WAN

Fecha de publicación: 11/07/2019

Importancia: Crítica

Recursos afectados:

- Todas las versiones de NetScaler SD-WAN 9.x;
- Todas las versiones de NetScaler SD-WAN 10.0.x, anteriores a 10.0.8;
- Todas las versiones de Citrix SD-WAN 10.1.x;

- Todas las versiones de Citrix SD-WAN 10.2.x, anteriores a 10.2.3.

Descripción:

Se han identificado varias vulnerabilidades en Citrix SD-WAN Center, NetScaler SD-WAN Center, Citrix SD-WAN Appliance y NetScaler SD-WAN Appliance. En conjunto, estas vulnerabilidades podrían dar lugar a que un atacante no autenticado ejecute comandos como *root* contra la consola de gestión de SD-WAN Center, o bien podrían utilizarse para obtener privilegios de *root* en el SD-WAN Appliance.

Solución:

- Actualizar a la versión 10.0.8 de NetScaler SD-WAN Center y NetScaler SD-WAN Appliance.
- Actualizar a la versión 10.2.3 de Citrix SD-WAN Center y Citrix SD-WAN Appliance.

Detalle:

Se han identificado las siguientes vulnerabilidades:

- Inyección de comandos no autenticados en Citrix SD-WAN Center, versiones 10.2.x anteriores a 10.2.3, y en NetScaler SD-WAN Center, versiones 10.0.x anteriores a 10.0.8. Se han reservado los identificadores CVE-2019-12985, CVE-2019-12986, CVE-2019-12987 y CVE-2019-12988 para esta vulnerabilidad.
- Salto de directorio en la escritura de archivos en Citrix SD-WAN Center, versiones 10.2.x anteriores a 10.2.3, y en NetScaler SD-WAN Center, versiones 10.0.x anteriores a 10.0.8. Se ha reservado el identificador CVE-2019-12990 para esta vulnerabilidad.
- Inyección de comandos autenticados en Citrix SD-WAN Center, versiones 10.2.x anteriores a 10.2.3, y en NetScaler SD-WAN Center, versiones 10.0.x anteriores a 10.0.8. Se ha reservado el identificador CVE-2019-12992 para esta vulnerabilidad.
- Inyection SQL no autenticada en Citrix SD-WAN Appliance, versiones 10.2.x anteriores a 10.2.3, y en NetScaler SD-WAN Appliance, versiones 10.0.x anteriores a 10.0.8. Se ha reservado el identificador CVE-2019-12989 para esta vulnerabilidad.
- Inyección de comandos autenticados en Citrix SD-WAN Appliance, versiones 10.2.x anteriores a 10.2.3, y en NetScaler SD-WAN Appliance, versiones 10.0.x anteriores a 10.0.8. Se ha reservado el identificador CVE-2019-12991 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Actualización de seguridad de Joomla! 3.9.10

Fecha de publicación: 11/07/2019

Importancia: Baja

Recursos afectados:

Joomla! CMS, versiones desde la 3.9.7 hasta la 3.9.9.

Descripción:

Joomla! ha publicado una nueva versión que soluciona una vulnerabilidad de criticidad baja en su núcleo, de tipo ejecución remota de código, además de otra vulnerabilidad introducida en la versión 3.9.9.

Solución:

Actualizar a la versión 3.9.10.

Detalle:

Esta vulnerabilidad, de tipo ejecución remota de código, se aprovecha de un filtrado inadecuado que permite a los usuarios autorizados crear campos personalizados para manipular las opciones de filtrado e inyectar una opción no validada. Además, la versión 3.9.10 soluciona otra vulnerabilidad, introducida en la versión 3.9.9, que afectaba a los estilos de plantillas de sitios web multilingÃ¤es.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en Juniper

Fecha de publicación: 11/07/2019

Importancia: Crítica

Recursos afectados:

- Juniper Networks Junos OS, versiones 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 16.1, 16.2, 17.1, 17.2, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4 y 19.1;
- Steel Belted Radius Carrier Edition versiones 8.4 y 8.5;
- Juniper Secure Analytics (JSA) Series;
- Junos Space versiones anteriores a 19.2R1.

Para más detalles sobre las versiones afectadas, consultar la sección de referencias.

Descripción:

Juniper ha publicado múltiples vulnerabilidades que afectan a sus productos Juniper Networks Junos OS, Steel Belted Radius Carrier Edition, Juniper Secure Analytics (JSA) Series y Junos Space.

Solución:

Actualizar los productos afectados: https://www.juniper.net/support/downloads/

Detalle:

Un usuario malintencionado que aprovechara alguna de las vulnerabilidades descritas, podría llegar a realizar las siguientes acciones en los productos afectados:

- denegación de servicio (DoS),

- ejecución remota de código,
- evadir los mecanismos de protección criptográfica,
- insertar datos en sesiones HTTPS, y posiblemente en otro tipo de sesiones protegidas por SSL o TLS,
- falsificar certificados,
- falsificar servidores SSL arbitrarios,
- comprometer la integridad del keystore BKS-V1,
- revelar detalles sobre la clave privada,
- introducir datos "invisibles" en una estructura firmada,
- obtener información sobre el valor k de la firma y, en última instancia, también del valor privado,
- obtener claves privadas,
- realizar ataques de distinción y de recuperación en texto plano,
- superar el mecanismo de protección criptográfico y descubrir una clave de autenticación,
- obtención o escalada de privilegios,
- enumeración de usuarios,
- ejecutar módulos locales PKCS#11 arbitrarios,
- obtener información sensible de clave privada,
- cierre inesperado del servicio,
- superar restricciones veriexec en Junos Os,
- divulgación de información,
- provocar que se reutilice esa conexión si este conoce la versión que no distingue entre mayúsculas/minúsculas de la contraseña correcta,
- desbordamiento de enteros y lectura fuera de límites,
- que libcurl escriba fuera de su búfer basado en memoria dinámica (heap),
- enviar peticiones de transferencia de red al host erróneo.

El listado de identificadores asociados a estas vulnerabilidades son los siguientes:

- Reservados:
  - Críticos y altos: CVE-2019-0049, CVE-2019-0052 y CVE-2019-0053.
  - Medios y bajos: CVE-2019-0046 y CVE-2019-0048.
- Asignados:
  - Críticos y altos: CVE-2016-1951, CVE-2014-1545, CVE-2013-5607, CVE-2018-1000613, CVE-2018-1000180, CVE-2018-5382, CVE-2016-1000352, CVE-2016-1000344, CVE-2016-1000342, CVE-2016-1000340, CVE-2016-1000338, CVE-2015-8325, CVE-2016-6515, CVE-2016-10009, CVE-2016-10010, CVE-2016-10012, CVE-2018-15504, CVE-2018-15505, CVE-2018-1060, CVE-2018-1061, CVE-2018-11237, CVE-2018-0732, CVE-2016-8615, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625, CVE-2018-10902, CVE-2019-5739 y CVE-2018-12327.
  - Medios y bajos: CVE-2016-1938, CVE-2009-3555, CVE-2009-2409, CVE-2009-2408, CVE-2016-1000346, CVE-2016-1000345, CVE-2016-1000341, CVE-2015-7940, CVE-2013-1624, CVE-2016-2427, CVE-2016-6210, CVE-2015-6564, CVE-2016-10011, CVE-2019-1559, CVE-2018-1729, CVE-2018-0739, CVE-2016-8616 y CVE-2019-6133.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad de inyección de plantillas en múltiples productos de Atlassian

Fecha de publicación: 12/07/2019

Importancia: Crítica

Recursos afectados:

Jira Server y Jira Data Center, versiones:

- desde 4.4.0 hasta la anterior a 7.6.14,
- desde 7.7.0 hasta la anterior a 7.13.5,
- desde 8.0.0 hasta la anterior a 8.0.3,
- desde 8.1.0 hasta la anterior a 8.1.2,
- desde 8.2.0 hasta la anterior a 8.2.3.

Descripción:

El investigador Daniil Dmitriev ha descubierto una vulnerabilidad de severidad crítica, de tipo inyección de plantillas del lado del servidor que podría permitir la ejecución remota de código.

Solución:

Actualizar a las siguientes versiones:

- 7.6.14,
- 7.13.5,
- 8.0.3,
- 8.1.2,
- 8.2.3.

Detalle:

Una vulnerabilidad de tipo inyección de plantillas del lado del servidor podría permitir a un atacante realizar ejecución remota de código. Se ha reservado el identificador CVE-2019-11581 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en Squid

Fecha de publicación: 15/07/2019

Importancia: Alta

Recursos afectados:

- Versiones afectadas de Squid:
  - Rama 2.x, todas las versiones;
  - Rama 3.x, hasta la versión 3.5.28;
  - Rama 4.x, hasta la versión 4.7.

Descripción:

Se han detectado cinco vulnerabilidades en múltiples versiones del servidor proxy Squid.

Solución:

Actualizar a la versión 4.8 para solucionar las vulnerabilidades.

Detalle:

- Las vulnerabilidades detectadas podrían permitir a un atacante remoto:
  - robar información,
  - ejecutar código y
  - generar una condición de denegación de servicio.

Se han reservado los identificadores CVE-2019-12854, CVE-2019-12529, CVE-2019-12525, CVE-2019-12527 y CVE-2019-13345 para estas vulnerabilidades.

Etiquetas: Actualización, Vulnerabilidad

Actualizaciones críticas en Oracle (julio 2019)

Fecha de publicación: 17/07/2019

Importancia: Crítica

Recursos afectados:

- Application Express, versiones 5.1, 18.2;
- Diagnostic Assistant, versiones anteriores a 2.12.36;
- Enterprise Manager Base Platform, versiones 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0;
- Enterprise Manager para Fusion Middleware, versiones 13.2, 13.3;
- Enterprise Manager para Virtualization, versiones 13.1, 13.2, 13.3;
- Enterprise Manager Ops Center, versiones 12.3.3, 12.4.0;
- Instantis EnterpriseTrack, versiones 17.1, 17.2, 17.3;
- JD Edwards EnterpriseOne Tools, versión 9.2;
- JD Edwards World Security, versiones A9.3, A9.3.1, A9.4;
- MICROS Retail XBRi Loss Prevention, versiones 10.8.0 - 10.8.3;
- MICROS Retail-J, versiones 12.1.0, 12.1.1, 12.1.2, 13.1;
- MySQL Enterprise Monitor, versiones 4.0.9 y anteriores, 8.0.14 y anteriores;
- MySQL Server, versiones 5.6.44 y anteriores, 5.7.26 y anteriores, 8.0.16 y anteriores;
- MySQL Workbench, versiones 8.0.16 y anteriores;
- Oracle Agile Engineering Data Management, versiones 6.2.0, 6.2.1;
- Oracle Agile PLM, versiones 9.3.3, 9.3.4, 9.3.5, 9.3.6;
- Oracle Application Testing Suite, versiones 13.1, 13.2, 13.3;
- Oracle Banking Platform, versiones 2.4.0 - 2.7.1;
- Oracle Berkeley DB, versiones 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23, 12.1.6.2.32;
- Oracle BI Publisher, versión 11.1.1.9.0;
- Oracle Business Intelligence Enterprise Edition, versiones 11.1.1.9.0, 12.2.1.4.0;
- Oracle Clusterware, versión 12.1.0.2.0;
- Oracle Communications Application Session Controller, versiones 3.7.1, 3.8.0;
- Oracle Communications Billing y Revenue Management, versiones 7.5, 12.0;
- Oracle Communications Converged Application Server, versiones 5.1, 7.0, 7.1;
- Oracle Communications Converged Application Server - Service Controller, versiones 6.0, 6.1;
- Oracle Communications Convergence, versión 3.0.2;
- Oracle Communications Diameter Signaling Router (DSR), versiones 8.0, 8.1, 8.2, 8.3;
- Oracle Communications EAGLE (Software), versiones 46.5, 46.6, 46.7;
- Oracle Communications Instant Messaging Server, versión 10.0.1.2.0;
- Oracle Communications Interactive Session Recorder, versiones 6.0, 6.1, 6.2;
- Oracle Communications Messaging Server, versiones 8.0.2, 8.1.0;
- Oracle Communications Online Mediation Controller, versión 6.1;
- Oracle Communications Unified, versión 8.0.0.2.0;
- Oracle Data Integrator, versión 12.2.1.3.0;
- Oracle Database Server, versiones 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c;
- Oracle Demantra Demy Management, versión 7.3.1.5.2;
- Oracle E-Business Suite, versiones 12.1.1 - 12.1.3, 12.2.3 - 12.2.8;
- Oracle Endeca Information Discovery Integrator, versión 3.2.0;
- Oracle Endeca Server, versión 7.7.0;
- Oracle Enterprise Manager Base Platform, versiones 12.1.0.5.0, 13.2.0.0.0, 13.3.0.0.0;
- Oracle Enterprise Repository, versión 12.1.3.0.0;
- Oracle Financial Services - Regulatory Reporting para Reserve Bank of India - Lombard Risk Integration Pack, versión 8.0.7;
- Oracle Financial Services - Regulatory Reporting para US Federal Reserve - Lombard Risk Integration Pack, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Analytical Applications Infrastructure, versiones 7.3.3 - 7.3.5, 8.0.2 - 8.0.8;
- Oracle Financial Services Analytical Applications Reconciliation Framework, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Asset Liability Management, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Basel Regulatory Capital Basic, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Data Foundation, versiones 8.0.4 - 8.0.8;
- Oracle Financial Services Data Integration Hub, versiones 8.0.5 - 8.0.7;
- Oracle Financial Services Funds Transfer Pricing, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Hedge Management y IFRS Valuations, versiones 8.0.4 - 8.0.7;

- Oracle Financial Services Institutional Performance Analytics, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Liquidity Risk Management, versiones 8.0.1, 8.0.2, 8.0.4, 8.0.5, 8.0.6;
- Oracle Financial Services Liquidity Risk Measurement y Management, versiones 8.0.7, 8.0.8;
- Oracle Financial Services Loan Loss Forecasting y Provisioning, versiones 8.0.2 - 8.0.7;
- Oracle Financial Services Market Risk Measurement y Management, versiones 8.0.5, 8.0.6, 8.0.8;
- Oracle Financial Services Price Creation y Discovery, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Profitability Management, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Regulatory Reporting para European Banking Authority, versiones 8.0.6, 8.0.7;
- Oracle Financial Services Regulatory Reporting para European Banking Authority - Integration Pack para Lombard Risk, versiones 8.0.6, 8.0.7;
- Oracle Financial Services Regulatory Reporting para US Federal Reserve, versiones 8.0.4 - 8.0.7;
- Oracle Financial Services Retail Customer Analytics, versiones 8.0.4 - 8.0.6;
- Oracle Financial Services Revenue Management y Billing, versiones 2.4.0.0, 2.4.0.1;
- Oracle FLEXCUBE Core Banking, versiones 5.2.0, 11.6.0, 11.7.0, 11.8.0;
- Oracle FLEXCUBE Enterprise Limits y Collateral Management, versiones 12.0, 12.1;
- Oracle FLEXCUBE Investor Servicing, versiones 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0, 14.1.0;
- Oracle FLEXCUBE Private Banking, versiones 12.0.1, 12.0.3, 12.1.0;
- Oracle FLEXCUBE Universal Banking, versiones 12.0.1 - 12.0.3, 12.1.0 - 12.4.0, 14.0.0 - 14.2.0;
- Oracle Global Lifecycle Management OPatchAuto, versiones anteriores a 12.2.0.1.14;
- Oracle GraalVM Enterprise Edition, versión 19.0.0;
- Oracle Hospitality Gift y Loyalty, versiones 9.0.0, 9.1.0;
- Oracle Hospitality Guest Access, versiones 4.2, 4.2.1;
- Oracle Hospitality Simphony, versión 18.2.1;
- Oracle Hospitality Suite8, versiones 8.9.6, 8.10.2, 8.11 - 8.14;
- Oracle HTTP Server, versiones 12.1.3.0.0, 12.2.1.3.0;
- Oracle Hyperion Planning, versión 11.1.2.4;
- Oracle Hyperion Workspace, versión 11.1.2.4;
- Oracle Identity Manager, versiones 11.1.2.3.0, 12.2.1.3.0;
- Oracle Insurance Allocation Manager para Enterprise Profitability, versión 8.0.8;
- Oracle Insurance Calculation Engine, versiones 9.7, 10.0, 10.1, 10.2;
- Oracle Insurance Data Foundation, versiones 8.0.4 - 8.0.7;
- Oracle Insurance IFRS 17 Analyzer, versiones 8.0.6, 8.0.7;
- Oracle Insurance Performance Insight, versión 8.0.7;
- Oracle Insurance Policy Administration J2EE, versiones 10.0, 10.1, 10.2, 11.0;
- Oracle Insurance Rules Palette, versiones 10.0, 10.1, 10.2, 11.0;
- Oracle Java SE, versiones 7u221, 8u212, 11.0.3, 12.0.1;
- Oracle Java SE Embedded, versión 8u211;
- Oracle Outside In Technology, versión 8.5.4;
- Oracle Retail Advanced Inventory Planning, versión 15.0;
- Oracle Retail Customer Management y Segmentation Foundation, versiones 16.0, 17.0, 18.0;
- Oracle Retail Financial Integration, versiones 14.0, 14.1, 15.0, 16.0;
- Oracle Retail Integration Bus, versiones 15.0, 16.0;
- Oracle Retail Order Broker, versiones 5.2, 15.0;
- Oracle Retail Order Management System, versión 5.0;
- Oracle Retail Predictive Application Server, versiones 14.0.3.26, 14.1.3.37, 15.0.3.100, 16.0;
- Oracle Retail Service Backbone, versión 16.0.1;
- Oracle Retail Xstore Office, versiones 7.0, 7.1;
- Oracle Retail Xstore Point of Service, versiones 7.0, 7.1, 15.0, 16.0, 17.0, 18.0;
- Oracle Security Service, versiones 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0;
- Oracle SOA Suite, versión 12.2.1.3.0;
- Oracle Solaris, versiones 10, 11.3, 11.4;
- Oracle Transportation Management, versión 6.3.7;
- Oracle Utilities Advanced Spatial y Operational Analytics, versión 2.7.0.1;
- Oracle Utilities Framework, versiones 4.3.0.2.0 - 4.3.0.6.0, 4.4.0.0.0;
- Oracle VM VirtualBox, versiones anteriores a 5.2.32, anterior a 6.0.10;
- Oracle WebCenter Sites, versión 12.2.1.3.0;
- Oracle WebLogic Server, versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0;
- PeopleSoft Enterprise FIN Project Costing, versión 9.2;
- PeopleSoft Enterprise PeopleTools, versiones 8.55, 8.56, 8.57;
- PeopleSoft Enterprise PT PeopleTools, versiones 8.55, 8.56, 8.57;
- Primavera Analytics, versión 18.8;
- Primavera Gateway, versiones 15.2, 16.2, 17.12, 18.8;
- Primavera Unifier, versiones 16.1, 16.2, 17.7 - 17.12, 18.8;
- Services Tools Bundle, versión 19.2;
- Siebel Applications, versiones 19.0 y anteriores;
- StorageTek Tape Analytics SW Tool, versión 2.3.0;
- Sun ZFS Storage Appliance Kit (AK), versión 8.8.3;
- System Utilities, versión 19.1;
- Tape Virtual Storage Manager GUI, versión 6.2.

Descripción:

Oracle ha publicado una actualización crítica con parches para corregir vulnerabilidades que afectan a múltiples productos.

Solución:

Aplicar los parches correspondientes según los productos afectados. La información para descargar las actualizaciones puede obtenerse del boletín de seguridad publicado por Oracle.

Detalle:

Esta actualización resuelve un total de 319 vulnerabilidades, algunas de las cuales son críticas. El detalle de las vulnerabilidades resueltas se puede consultar en el enlace de Oracle de la sección de Referencias.

Etiquetas: Actualización, Java, Oracle, Virtualización, Vulnerabilidad

---

Vulnerabilidad de omisión de seguridad en Windows Defender Application Control (WDAC)

Fecha de publicación: 17/07/2019

Importancia: Alta

Recursos afectados:

- PowerShell Core versiones 6.1 y 6.2.

Descripción:

Microsoft ha corregido una vulnerabilidad fuera de ciclo, que afectaba a su producto PowerShell Core.

Solución:

- PowerShell Core versión 6.1 actualizar a la versión 6.1.5
- PowerShell Core versión 6.2 actualizar a la versión 6.2.2

Detalle:

Una vulnerabilidad de omisión de seguridad en Windows Defender Application Control (WDAC) podría permitir a un atacante, con permisos de administración, eludir el modo de lenguaje restringido de PowerShell Core y acceder a los recursos de forma involuntaria. Se ha reservado el identificador CVE-2019-1167 para esta vulnerabilidad.

Etiquetas: Actualización, Microsoft, Vulnerabilidad

Vulnerabilidad de omisión de acceso en el core de Drupal

Fecha de publicación: 18/07/2019

Importancia: Alta

Recursos afectados:

Versión 8.7.4.

Descripción:

Se ha descubierto una vulnerabilidad de omisión de acceso en el *core* de Drupal.

Solución:

Si el sitio web está ejecutando Drupal 8.7.4, actualizar a la versión 8.7.5. Para sitios web con el módulo *Workspaces* habilitado, el archivo *update.php* debe ejecutarse para garantizar la necesaria limpieza de la caché. Si hay una caché de proxy inverso o una red de distribución de contenidos (CDN), también es aconsejable realizar la limpieza de caché en ellos.

Detalle:

En Drupal 8.7.4, cuando se activa el módulo experimental *Workspaces*, se crea una condición de omisión de acceso. Se ha reservado el identificador CVE-2019-6342 para esta vulnerabilidad.

Etiquetas: Actualización, CMS, Vulnerabilidad

Múltiples vulnerabilidades en Jenkins

Fecha de publicación: 18/07/2019

Importancia: Alta

Recursos afectados:

- Jenkins Weekly, versiones 2.185 y anteriores.
- Jenkins LTS, versiones 2.176.1 y anteriores.

Descripción:

Jenkins ha publicado 3 vulnerabilidades, una de criticidad alta y dos clasificadas como medias. La explotación de alguna de estas vulnerabilidades podría permitir realizar ataques *Cross-site request forgery* (CSRF), escribir archivos de forma arbitrario o acceso no autorizado a vista de fragmentos.

Solución:

- Jenkins Weekly actualizar a la versión 2.186.
- Jenkins LTS versión 2.176.2.

Detalle:

- En la vulnerabilidad de severidad alta, debido a que los tokens en Jenkins solo verifican la autenticación del usuario y la dirección IP, un atacante podría obtener un token de otro usuario y realizar ataques *Cross-site request forgery* (CSRF), siempre y cuando la dirección IP de la víctima permanezca inalterada. Se ha asignado el identificador CVE-2019-10353 para esta vulnerabilidad.
- Para el resto de vulnerabilidades se han asignado los identificadores CVE-2019-10352 y CVE-2019-10354.

Etiquetas: Actualización, Vulnerabilidad

Múltiples vulnerabilidades en dispositivos Cisco

Fecha de publicación: 18/07/2019

Importancia: Crítica

Recursos afectados:

- Cisco Vision Dynamic Signage Director, versiones:
  - 5.0 y anteriores;
  - 6.0;
  - 6.1.
- Cisco FindIT Network Manager y Cisco FindIT Network Probe versión 1.1.4, si utilizan las imágenes virtuales suministradas por Cisco.
- Cisco IOS Access Points Major Software configurados para 802.11r FT, versiones:
  - 8.0 y anteriores;
  - 8.1;
  - 8.2;
  - 8.3;
  - 8.4;
  - 8.5;
  - 8.6;
  - 8.7.

Descripción:

Cisco ha descubierto tres vulnerabilidades, una de severidad crítica y dos de severidad alta, que afectan a múltiples productos. Un atacante remoto, sin autenticación, podría omitir la autenticación, acceder a una cuenta con privilegios de *root* o generar una condición de denegación de servicio.

Solución:

- Cisco Vision Dynamic Signage Director, versiones:
  - 5.0 y anteriores, actualizar a 5.0sp9;
  - 6.0 y 6.1, actualizar a 6.1sp3.
- Cisco FindIT Network Manager y Cisco FindIT Network Probe versión 1.1.4, actualizar a la versión 2.0.
- Cisco IOS Access Points Major Software configurados para 802.11r FT:
  - versiones 8.0 y anteriores, 8.1 y 8.2, actualizar a la versión 8.2.170.0;
  - versión 8.3, actualizar a la versión 8.3.150.0;
  - versiones 8.4 y 8.5, actualizar a la versión 8.5.131.0;
  - versiones 8.6 y 8.7, actualizar a la versión 8.8.100.0.

Detalle:

- La vulnerabilidad de severidad crítica afecta a la interfaz REST API de Cisco Vision Dynamic Signage Director Software. Esta se debe a una validación insuficiente en las peticiones HTTP. Un atacante remoto, sin autenticación, podría enviar un paquete HTTP, especialmente generado, y realizar acciones arbitrarias con privilegios administrativos en el sistema. Se ha asignado el identificador CVE-2019-1917 para esta vulnerabilidad.
- Una vulnerabilidad de severidad alta se debe a la presencia de una cuenta con credenciales estáticas en el sistema operativo Linux subyacente. Un atacante podría acceder a dicha cuenta que tiene privilegios de *root*. Se ha asignado el identificador CVE-2019-1919 para esta vulnerabilidad.
- Una vulnerabilidad, de severidad alta, se debe a una completa falta en la condición de manejo de errores en las peticiones de autenticación del cliente, enviadas a la interfaz configurada para FT. Un atacante adyacente podría enviar una petición de autenticación, especialmente generada a la interfaz, pudiendo generar una condición de denegación de servicio (DoS). Se ha asignado el identificador CVE-2019-1920 para esta vulnerabilidad.

Etiquetas: Actualización, Cisco, Vulnerabilidad

Vulnerabilidad de ejecución remota de código en Palo Alto PAN-OS

Fecha de publicación: 19/07/2019

Importancia: Crítica

Recursos afectados:

- PAN-OS 7.1.18 y anteriores.
- PAN-OS 8.0.11 y anteriores.
- PAN-OS 8.1.2 y anteriores.

Descripción:

Palo Alto ha publicado una vulnerabilidad de severidad crítica, que podría permitir a un atacante no autenticado ejecutar código arbitrario.

Solución:

Palo Alto recomienda actualizar sus productos a las siguientes versiones:

- PAN-OS 7.1.19 o superior.
- PAN-OS 8.0.12 o superior.
- PAN-OS 8.1.3 o superior.

Detalle:

La vulnerabilidad, de ejecución remota de código (RCE), podría permitir a un atacante no autenticado ejecutar código arbitrario. Se ha reservado el identificador CVE-2019-1579 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Vulnerabilidad en servidores ProFTPD

Fecha de publicación: 25/07/2019

Importancia: Crítica

Recursos afectados:

Versiones 1.3.6 y anteriores.

Descripción:

El investigador Tobias MÃ¤del ha detectado una vulnerabilidad de severidad crítica en el módulo *mod_copy* de los servidores ProFTPD. Un atacante remoto, sin autenticación, podría ejecutar código o revelar información.

Solución:

No se ha publicado una solución en forma de nueva versión o actualización para esta vulnerabilidad. Se recomienda permanecer a la espera ante una posible actualización.

- Como medida de mitigación se recomienda deshabilitar el modulo *mod_copy*.
- Se ha desarrollado una corrección que puede consultarse en el Bug Tracker del repositorio de git.
- En el caso particular de Debian, se ha desarrollado un parche disponible únicamente en la versión 1.3.6-6 inestable (*Release sid*).

Detalle:

Una vulnerabilidad en el modulo *mod_copy*, encargado de gestionar la copia de archivos entre directorios, podría permitir a un atacante remoto, sin autenticación, ejecutar código o revelar información. Se ha asignado el identificador CVE-2019-12815 para esta vulnerabilidad.

Etiquetas: Linux, Vulnerabilidad

Vulnerabilidad en Network Time Protocol (NTP)

Fecha de publicación: 25/07/2019

Importancia: Alta

Recursos afectados:

- Productos F5:
  - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), versiones:
    - 15.0.0;
    - desde la 14.0.0 hasta la 14.1.0;
    - desde la 13.1.0 hasta la 13.1.1;
    - desde la 12.1.0 hasta la 12.1.4;
    - desde la 11.5.2 hasta la 11.6.4;
  - Enterprise Manager. versión 3.1.1;
  - BIG-IQ Centralized Management, versiones:
    - desde la 6.0.0 hasta la 6.1.0;
    - desde la 5.1.0 hasta la 5.4.0;
  - F5 iWorkflow, versión 2.3.0;
  - Traffix SDC, desde la versión 5.0.0 hasta la versión 5.1.0.
- Red Hat Enterprise versiones 5, 6 y 7

Descripción:

Se ha detectado una vulnerabilidad de criticidad alta que afecta al protocolo NTP. Un atacante remoto podría acceder a los recursos, modificar archivos o generar una condición de denegación de servicio en el sistema.

Solución:

No se ha publicado una solución en forma de parche o actualización para esta vulnerabilidad, tampoco se han publicado indicaciones para mitigar la vulnerabilidad, por ello recomendamos permanecer a la espera ante una posible actualización.

Detalle:

Network Time Protocol (NTP), tal y como se especifica en el RFC 5905, utiliza el puerto 123 incluso para los modos en los que no se requiere un número de puerto fijo, lo que facilita a los atacantes remotos la realización de ataques fuera de ruta. Un atacante remoto podría acceder a los recursos, modificar archivos o generar una condición de denegación de servicio en el sistema. Se ha asignado le identificador CVE-2019-11331 para esta vulnerabilidad.

Etiquetas: Linux, Vulnerabilidad

Vulnerabilidad en Exim

Fecha de publicación: 26/07/2019

Importancia: Alta

Recursos afectados:

Exim, versiones desde la 4.85 hasta la 4.92.

Descripción:

El investigador Jeremy Harris ha descubierto una vulnerabilidad de criticidad alta. Un atacante, local o remoto, podría ejecutar programas con privilegios de *root*.

Solución:

Actualizar Exim a la versión 4.92.1

Detalle:

La vulnerabilidad se debe a una gestión indebida de la expansión *${sort}* para ítems. Un atacante, remoto o local, podría ejecutar programas con privilegios de *root* en sistemas que empleen la expansión *${sort}* para ítems en sus configuraciones. Se ha asignado el identificador CVE-2019-13917 para esta vulnerabilidad.

Etiquetas: Actualización, Vulnerabilidad

Ataque de inyección XXE en Daeja ViewONE de IBM

Fecha de publicación: 29/07/2019

Importancia: Alta

Recursos afectados:

Daeja ViewONE Virtual, desde la versión 5.0 hasta la 5.0.6.

Descripción:

IBM ha publicado una vulnerabilidad de criticidad alta en Daeja ViewONE Professional, Standard y Virtual. Un atacante remoto podría revelar información sensible o generar una condición de denegación de servicio.

Solución:

IBM ha publicado dos parches para solucionar la vulnerabilidad:

- Daeja ViewONE Virtual 5.0.5 iFix 14
- Daeja ViewONE Virtual 5.0.6 iFix 2

Detalle:

Daeja ViewONE Virtual es vulnerable a un ataque de inyección XML *External Entity* (XXE) al procesar datos XML. Un atacante remoto podría exponer información sensible o consumir recursos de memoria, pudiendo generar una condición de denegación de servicio. Se ha reservado el identificador CVE-2019-4456 para esta vulnerabilidad.

Etiquetas: Actualización, IBM, Vulnerabilidad